ID: 562044
Sample Name: HSBC Bank Swift Copy.pdf.exe
Cookbook: default.jbs
Time: 10:55:25
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

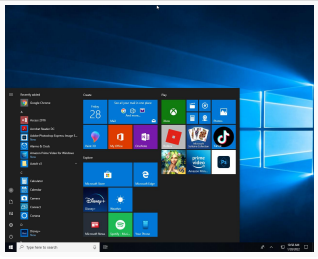
Windows Analysis Report

HSBC Bank Swift Copy.pdf.exe

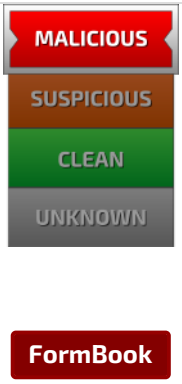
Overview

General Information

Sample Name:	HSBC Bank Swift Copy.pdf.exe
Analysis ID:	562044
MD5:	76b0f4441930d3..
SHA1:	0b28664196cd55..
SHA256:	3cc59342fdbb5a…
Tags:	exe Formbook HSBC
Infos:	



Detection



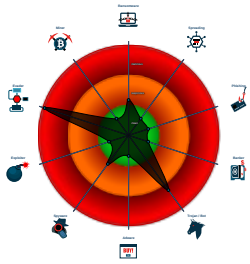
FormBook

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Sigma detected: Suspicious Double…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- Antivirus detection for URL or domain
- Sigma detected: Suspect Svchost A…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- HSBC Bank Swift Copy.pdf.exe (PID: 4712 cmdline: "C:\Users\user\Desktop\HSBC Bank Swift Copy.pdf.exe" MD5: 76B0F4441930D3F2F480830681C426E7)
  - HSBC Bank Swift Copy.pdf.exe (PID: 4824 cmdline: C:\Users\user\Desktop\HSBC Bank Swift Copy.pdf.exe MD5: 76B0F4441930D3F2F480830681C426E7)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - svchost.exe (PID: 5976 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
        - cmd.exe (PID: 4384 cmdline: /c del "C:\Users\user\Desktop\HSBC Bank Swift Copy.pdf.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5464 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - explorer.exe (PID: 4524 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.loj-kits.xyz/rexd/"
  ],
  "decoy": [
    "xn--2es77o3w1bruk.mobi",
    "cotesaintetienne.com",
    "newlifefoursquaremcpherson.com",
    "solutions-consulting.biz",
    "chsico.com",
    "demeet.xyz",
    "eiruhguijire.store",
    "realestatemoda.com",
    "amr-fire.net",
    "99v.one",
    "altdaita.com",
    "showerbeast.com",
    "nsfone.com",
    "doanhnhanvietnam.info",
    "xn--transfpanou-39a.com",
    "invitiz.com",
    "chifaebio.xyz",
    "footprint-farm.com",
    "onlinenurseprograms.com",
    "tigeratlspa.com",
    "troublewatermelon.space",
    "juvesti.com",
    "hunnii.one",
    "collective4choice.com",
    "casino-mate1.com",
    "hairandspa-aimer-kadsume.com",
    "pointconstructionservices.com",
    "savagereviews.xyz",
    "zhuangmengmeng.com",
    "gicaredocs.com",
    "victori-jaya.com",
    "purifilt.net",
    "live9words.com",
    "x-teknoloji.com",
    "thelocalworkers.com",
    "nalainteriores.com",
    "dream-mart.tech",
    "maretta.info",
    "empowermindbodystudios.com",
    "creativenft.xyz",
    "remembertheabbeygate.com",
    "whistlergardencenter.com",
    "jbmfg.net",
    "tangerinecave.com",
    "60thstreetdesserts.com",
    "mxcpgj.com",
    "nguoidantocvungcao.xyz",
    "snowjamproductiosmedia.com",
    "schencklab.com",
    "sousouhenansheng.com",
    "quirkysoul39.com",
    "digitaleclipsegames.com",
    "hayesvalleycondo409.com",
    "ceremonydesigncompany.com",
    "essaispsoriasisenfants-ca.com",
    "borhanmarket.com",
    "aerbounce.com",
    "primebradescocadastro.com",
    "bupis44.info",
    "optmsg.com",
    "khukhuanphongkham.com",
    "bunnymoorellc.com",
    "tminus-10.com",
    "mytechmadesimple.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.378377402.0000000000E50000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000C.00000002.378377402.0000000000E50000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000C.00000002.378377402.0000000000E50000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
0000000C.00000002.378466176.00000000011A0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000C.00000002.378466176.00000000011A0000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.0.HSBC Bank Swift Copy.pdf.exe.400000.8.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
12.0.HSBC Bank Swift Copy.pdf.exe.400000.8.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
12.0.HSBC Bank Swift Copy.pdf.exe.400000.8.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cc9:$sqlite3step: 68 34 1C 7B E1 • 0x15ddc:$sqlite3step: 68 34 1C 7B E1 • 0x15cf8:$sqlite3text: 68 38 2A 90 C5 • 0x15e1d:$sqlite3text: 68 38 2A 90 C5 • 0x15d0b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e33:$sqlite3blob: 68 53 D8 7F 8C
12.0.HSBC Bank Swift Copy.pdf.exe.400000.6.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
12.0.HSBC Bank Swift Copy.pdf.exe.400000.6.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 24 entries				

Sigma Overview

System Summary

Sigma detected: Suspicious Double Extension

Sigma detected: Suspect Svchost Activity

Sigma detected: Suspicious Svchost Process

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd delete

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

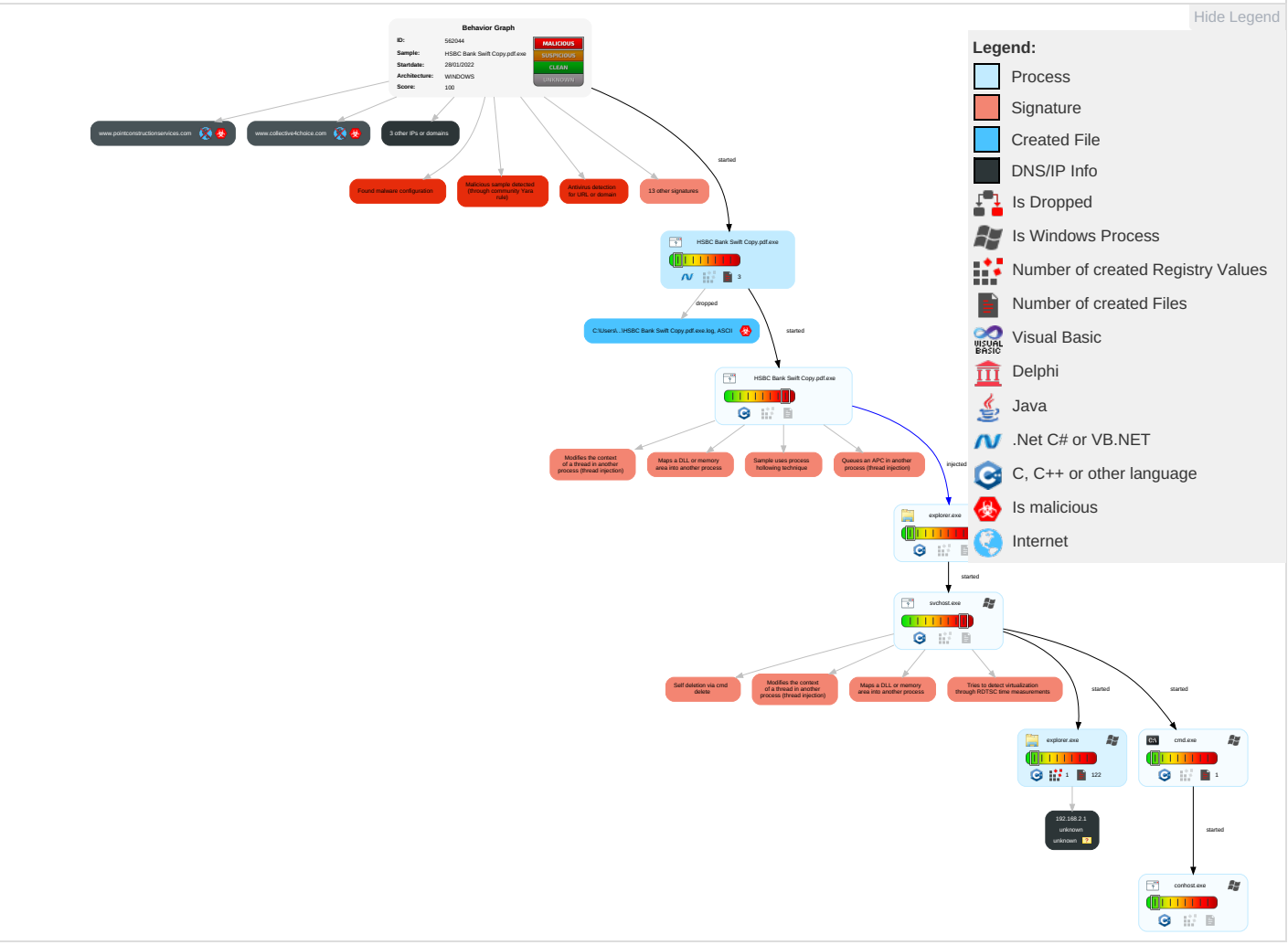
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	4 1 2 Process Injection	1 1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 4 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	4 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	4 1 2 Process Injection	NTDS	4 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 2 Obfuscated Files or Information	Cached Domain Credentials	1 1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 File Deletion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

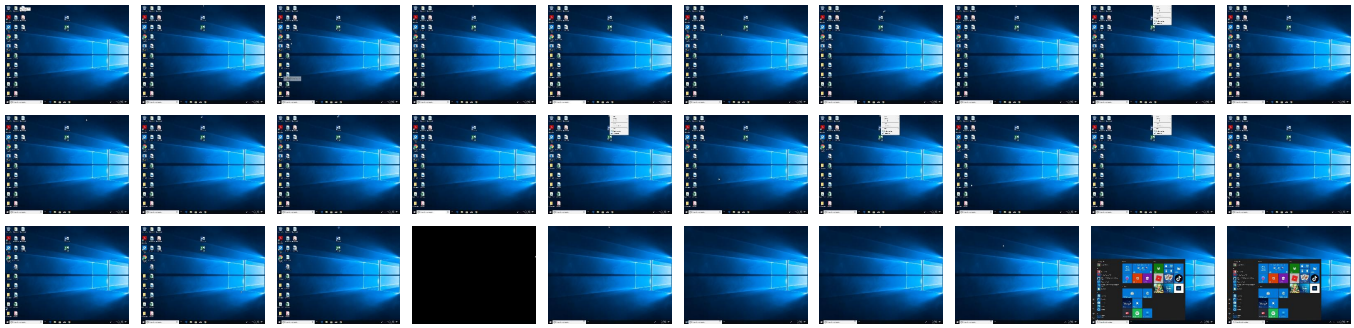
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
HSBC Bank Swift Copy.pdf.exe	32%	Virustotal		Browse
HSBC Bank Swift Copy.pdf.exe	49%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
HSBC Bank Swift Copy.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.0.HSBC Bank Swift Copy.pdf.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.2.HSBC Bank Swift Copy.pdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.0.HSBC Bank Swift Copy.pdf.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.0.HSBC Bank Swift Copy.pdf.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.chifaebio.xyz	0%	Avira URL Cloud	safe	
http://www.loj-kits.xyz	0%	Avira URL Cloud	safe	
http://www.mxcpgj.com	0%	Avira URL Cloud	safe	
http://www.bupis44.infoReferer:	0%	Avira URL Cloud	safe	
http://www.pointconstructionservices.comReferer:	0%	Avira URL Cloud	safe	
http://www.nalainteriores.com/rexd/www.essaispsoriasisenfants-ca.com	0%	Avira URL Cloud	safe	
http://www.invitiz.com/rexd/www.primebradescocadastro.com	0%	Avira URL Cloud	safe	
http://www.doanhnhanvietnam.infoReferer:	0%	Avira URL Cloud	safe	
http://www.primebradescocadastro.com/rexd/	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.solutions-consulting.biz	0%	Avira URL Cloud	safe	
http://www.chifaebio.xyz/rexd/	0%	Avira URL Cloud	safe	
http://www.doanhnhanvietnam.info/rexd/	100%	Avira URL Cloud	malware	
http://www.tminus-10.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.primebradescocadastro.com	0%	Avira URL Cloud	safe	
http://www.invitiz.com/rexd/	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.tminus-10.com/rexd/www.loj-kits.xyz	0%	Avira URL Cloud	safe	
http://www.invitiz.comReferer:	0%	Avira URL Cloud	safe	
http://www.essaispsoriasisenfants-ca.comReferer:	0%	Avira URL Cloud	safe	
http://www.hairandspa-aimer-kadsume.com/rexd/	100%	Avira URL Cloud	malware	
http://www.pointconstructionservices.com/rexd/www.amr-fire.net	0%	Avira URL Cloud	safe	
http://components.groove.net/Groove/Components/Root.osd? Package=net.groove.Groove.Tools.System.Groov	0%	Avira URL Cloud	safe	
http://www.mxcpgj.comReferer:	0%	Avira URL Cloud	safe	
http://www.amr-fire.net/rexd/	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.collective4choice.comReferer:	0%	Avira URL Cloud	safe	
http://www.bupis44.info/rexd/www.solutions-consulting.biz	100%	Avira URL Cloud	malware	
www.loj-kits.xyz/rexd/	100%	Avira URL Cloud	malware	
http://www.chifaebio.xyzReferer:	0%	Avira URL Cloud	safe	
http://www.doanhnhanvietnam.info	0%	Avira URL Cloud	safe	
http://www.nalainteriores.com	0%	Avira URL Cloud	safe	
http://www.collective4choice.com/rexd/www.bupis44.info	100%	Avira URL Cloud	malware	
http://blog.iandreev.com/	0%	Avira URL Cloud	safe	
http://www.collective4choice.com/rexd/	100%	Avira URL Cloud	malware	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.loj-kits.xyz/rexd/www.chifaebio.xyz	100%	Avira URL Cloud	malware	
http://www.solutions-consulting.biz/rexd/www.hairandspa-aimer-kadsume.com	0%	Avira URL Cloud	safe	
http://components.groove.net/Groove/Components/SystemComponents/SystemComponents.osd? Package=net.gro	0%	Avira URL Cloud	safe	
http://www.amr-fire.net	0%	Avira URL Cloud	safe	
http://www.nalainteriores.comReferer:	0%	Avira URL Cloud	safe	
http://www.essaispsoriasisenfants-ca.com/rexd/	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.doanhnhanvietnam.info/rexd/www.invitiz.com	100%	Avira URL Cloud	malware	
http://blog.iandreev.com/AClick	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.essaispsoriasisenfants-ca.com	0%	Avira URL Cloud	safe	
http://www.hairandspa-aimer-kadsume.comReferer:	0%	Avira URL Cloud	safe	
http://www.live9words.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.bupis44.info/rexd/	100%	Avira URL Cloud	malware	
http://www.hairandspa-aimer-kadsume.com	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.loj-kits.xyz/rexd/	100%	Avira URL Cloud	malware	
http://www.pointconstructionservices.com	0%	Avira URL Cloud	safe	
http://www.amr-fire.net/rexd/www.collective4choice.com	0%	Avira URL Cloud	safe	
http://www.live9words.com/rexd/	0%	Avira URL Cloud	safe	
http://www.essaispsoriasisenfants-ca.com/rexd/www.doanhnhanvietnam.info	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.hairandspa-aimer-kadsume.com/rexd/www.tminus-10.com	100%	Avira URL Cloud	malware	
http://www.chifaebio.xyz/rexd/www.mxcpgj.com	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.nalainteriores.com/rexd/	0%	Avira URL Cloud	safe	
http://blog.iandreev.com	0%	Avira URL Cloud	safe	
http://www.tminus-10.comReferer:	0%	Avira URL Cloud	safe	
http://www.pointconstructionservices.com/rexd/	0%	Avira URL Cloud	safe	
http://www.primebradescocadastro.comReferer:	0%	Avira URL Cloud	safe	
http://www.tminus-10.com/rexd/	0%	Avira URL Cloud	safe	
http://crl.verisign.6	0%	Avira URL Cloud	safe	
http://www.collective4choice.com	0%	Avira URL Cloud	safe	
http://www.loj-kits.xyzReferer:	0%	Avira URL Cloud	safe	
http://www.solutions-consulting.bizReferer:	0%	Avira URL Cloud	safe	
http://www.live9words.comReferer:	0%	Avira URL Cloud	safe	
http://www.solutions-consulting.biz/rexd/	0%	Avira URL Cloud	safe	
http://www.amr-fire.netReferer:	0%	Avira URL Cloud	safe	
http://www.primebradescocadastro.com/rexd/www.live9words.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.bupis44.info	100%	Avira URL Cloud	malware	
http://www.mxcpgj.com/rexd/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comrsiva	0%	URL Reputation	safe	
http://www.invitiz.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdiao	0%	Avira URL Cloud	safe	
http://www.mxcpgj.com/rexd/www.nalainteriores.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pointconstructionservices.com	34.102.136.180	true	true		unknown
d1g9pg5cncourf.cloudfront.net	13.225.39.103	true	false		high
www.amr-fire.net	unknown	unknown	true		unknown
www.pointconstructionservices.com	unknown	unknown	true		unknown
www.collective4choice.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.loj-kits.xyz/rexd/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.chifaebio.xyz	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.loj-kits.xyz	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mxcpgj.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bupis44.infoReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.pointconstructionservices.comReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nalainteriores.com/rexd/www.essaispsoriasisenfants-ca.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false		high
http://www.invitiz.com/rexd/www.primebradescocadastro.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.doanhnhanvietnam.infoReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.primebradescocadastro.com/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.solutions-consulting.biz	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.chifaebio.xyz/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.doanhnhanvietnam.info/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.tminus-10.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.primebradescocadastro.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.invitiz.com/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tminus-10.com/rexd/www.loj-kits.xyz	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.invitiz.comReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 0000000E.00000000.35127031 6.0000000006840000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00E.00000000.335111009.0000000006840000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000E.00000000.418985985.000000 0006870000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 0000000E.0000 0000.314141640.0000000006840000.00000004 .00000001.00020000.00000000.sdmp	false		high

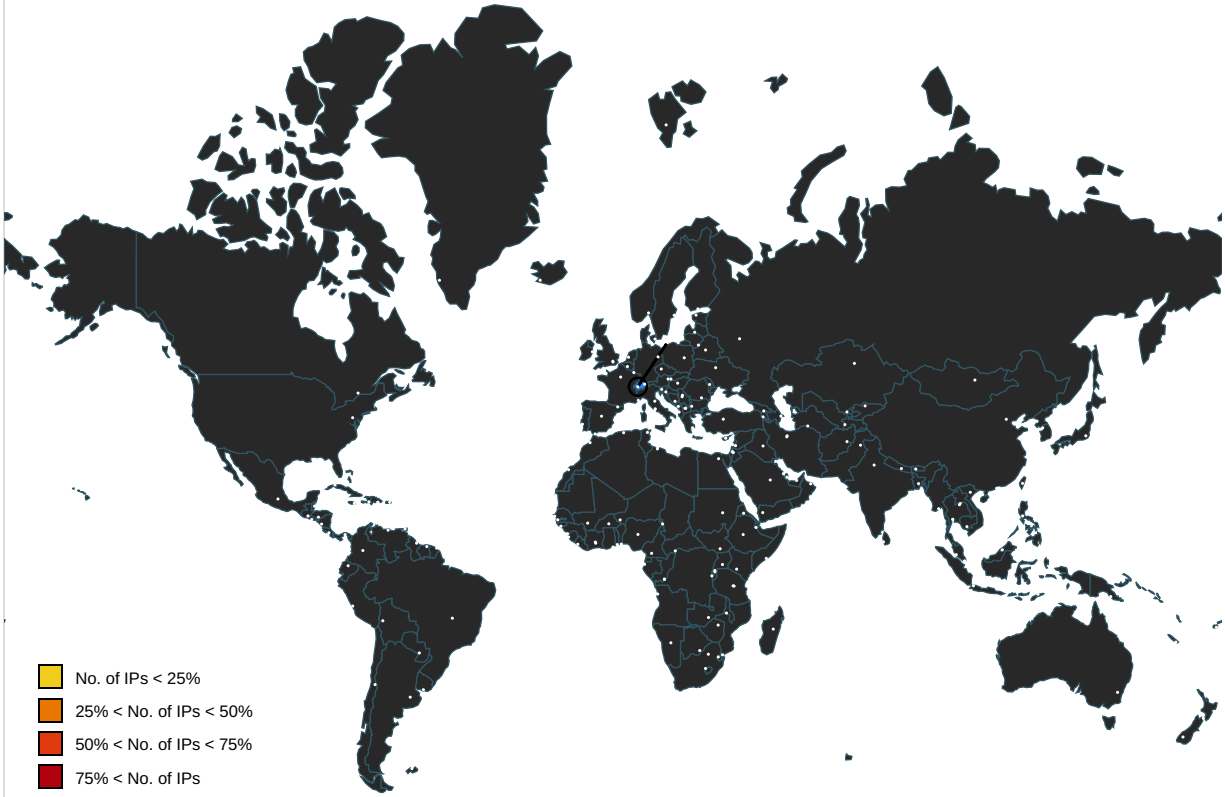
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.essaispsoriasisenfants-ca.comReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hairandspa-aimer-kadsume.com/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.pointconstructionservices.com/rexd/www.amr-fire.net	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://components.groove.net/Groove/Components/Root.osd?Package=net.groove.Groove.Tools.System.Groov	explorer.exe, 0000001D.00000002.54581158 1.00007FFF94839000.00000002.00000001.010 00000.00000008.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mxcpgj.comReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.amr-fire.net/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false		high
http://www.collective4choice.comReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bupis44.info/rexd/www.solutions-consulting.biz	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.chifaebio.xyzReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.doanhnhanvietnam.info	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nalainteriores.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.collective4choice.com/rexd/www.bupis44.info	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.fontbureau.com/designersG	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false		high
http://blog.iandreev.com/	HSBC Bank Swift Copy.pdf.exe	false	• Avira URL Cloud: safe	unknown
http://www.collective4choice.com/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.fontbureau.com/designers/?	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.loj-kits.xyz/rexd/www.chifaebio.xyz	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.solutions-consulting.biz/rexd/www.hairandspa-aimer-kadsume.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false		high
http://components.groove.net/Groove/Components/SystemComponents/SystemComponents.osd?Package=net.gro	explorer.exe, 0000001D.00000002.54581158 1.00007FFF94839000.00000002.00000001.010 00000.00000008.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.amr-fire.net	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nalainteriores.comReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.essaispsoriasisenfants-ca.com/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	HSBC Bank Swift Copy.pdf.exe, 00000000.00000002.309728380.00000000072E2000.00000004.00000800.00020000.00000000.sdmp, HSBC Bank Swift Copy.pdf.exe, 00000000.00000003.26474646.000000000199C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.doanhnhanvietnam.info/rexd/www.invitiz.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://blog.iandreev.com/AClick	HSBC Bank Swift Copy.pdf.exe	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	HSBC Bank Swift Copy.pdf.exe, 00000000.00000002.309728380.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.essaispsoriasisenfants-ca.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hairandspa-aimer-kadsume.comReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.live9words.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bupis44.info/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.hairandspa-aimer-kadsume.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	HSBC Bank Swift Copy.pdf.exe, 00000000.00000002.309728380.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	HSBC Bank Swift Copy.pdf.exe, 00000000.00000002.309728380.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	HSBC Bank Swift Copy.pdf.exe, 00000000.00000002.309728380.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.loj-kits.xyz/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.pointconstructionservices.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.amr-fire.net/rexd/www.collective4choice.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.live9words.com/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.essaispsoriasisenfants-ca.com/rexd/www.doanhnhanvietnam.info	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	HSBC Bank Swift Copy.pdf.exe, 00000000.00000002.309728380.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	HSBC Bank Swift Copy.pdf.exe, 00000000.00000002.309728380.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.hairandspa-aimer-kadsume.com/rexd/www.tminus-10.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.chifaebio.xyz/rexd/www.mxcpgj.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	HSBC Bank Swift Copy.pdf.exe, 00000000.00000002.309728380.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	HSBC Bank Swift Copy.pdf.exe, 00000000.00000002.309728380.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	HSBC Bank Swift Copy.pdf.exe, 00000000.00000002.309728380.00000000072E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.nalainteriores.com/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://blog.iandreev.com	HSBC Bank Swift Copy.pdf.exe	false	• Avira URL Cloud: safe	unknown
http://www.tminus-10.comReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pointconstructionservices.com/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.primebradescocadastro.comReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tminus-10.com/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.verisign.6	explorer.exe, 0000001D.00000000.50632194 5.0000000009A2B000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 01D.00000003.502118090.0000000009A06000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001D.00000003.502938145.000000 0009A2A000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 0000001D.0000 0003.500906015.0000000009A06000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 0000001D.00000003.505028040.0000000009A2A0 00.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000001D.00000003.504397605.000 0000009A2A000.00000004.00000020.00020000 .00000000.sdmp, explorer.exe, 0000001D.0 0000003.503803391.0000000009A08000.00000 004.00000020.00020000.00000000.sdmp, exp lorer.exe, 0000001D.00000000.513670120.0 000000009A2B000.00000004.00000020.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.collective4choice.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.loj-kits.xyzReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.solutions-consulting.bizReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.live9words.comReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.solutions-consulting.biz/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.amr-fire.netReferer:	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false		high
http:// www.primebradescocadastro.com/rexd/www.live9word s.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.bupis44.info	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.mxcpgj.com/rexd/	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comrsiva	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.307291346.0000000001997000.00000 004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	HSBC Bank Swift Copy.pdf.exe, 00000000.0 0000002.309728380.00000000072E2000.00000 004.00000800.00020000.00000000.sdmp	false		high
http://www.invitiz.com	explorer.exe, 0000001D.00000002.54001035 6.0000000009913000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comdiao	HSBC Bank Swift Copy.pdf.exe, 00000000.00000002.307291346.0000000001997000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mxcpgj.com/rexd/www.nalainteriores.com	explorer.exe, 0000001D.00000002.54001035.0000000009913000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562044
Start date:	28.01.2022
Start time:	10:55:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HSBC Bank Swift Copy.pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/1@3/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 69.1% (good quality ratio 64.5%) • Quality average: 71.3% • Quality standard deviation: 30.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SearchUI.exe, dllhost.exe, backgroundTaskHost.exe, BackgroundTransferHost.exe, WerFault.exe, ShellExperienceHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, mobsync.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 20.189.173.22
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, onedsblobprdwus17.westus.cloudapp.azure.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtEnumerateValueKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:56:47	API Interceptor	1x Sleep call for process: HSBC Bank Swift Copy.pdf.exe modified
10:58:02	API Interceptor	82x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HSBC Bank Swift Copy.pdf.exe.log

Process:	C:\Users\user\Desktop\HSBC Bank Swift Copy.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.450297231968026
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	HSBC Bank Swift Copy.pdf.exe
File size:	770048
MD5:	76b0f4441930d3f2f480830681c426e7
SHA1:	0b28664196cd55adcc7b82647602db984dd49f61
SHA256:	3cc59342fdbb5aa332f7d99216ac3f1ede121e0752e5aaff260e16432c23908d
SHA512:	63d7cbcaa3b46cce81727e5baa82e5daa055b3ad95d1fb14086bf2dd2bbd2811400b15e9231a18dc5ab1771c18f2047077baaefe8b970463da947fc650d32884
SSDEEP:	12288:9vlo9vY4GuoGLzezhMXxJYpfuRss38iZ:foFY4GuoG3ezhMXxJO/c
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....2.a.....0..... .....@.. .... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4bd4ea
Entrypoint Section:	.text

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61F332EA [Fri Jan 28 00:03:54 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbd498	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbe000	0x5cc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xbd360	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbb4f0	0xbb600	False	0.488747706805	data	6.45404426837	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0x5cc	0x600	False	0.427083333333	data	4.13288039483	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xbe090	0x33c	data		
RT_MANIFEST	0xbe3dc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	1.0.0.0
InternalName	RuntimePropertyIn.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	OthelloCS
ProductVersion	1.0.0.0
FileDescription	OthelloCS
OriginalFilename	RuntimePropertyIn.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-10:58:40.442828	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49861	34.102.136.180	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 10:58:40.275278091 CET	51919	53	192.168.2.7	8.8.8.8
Jan 28, 2022 10:58:40.305191040 CET	53	51919	8.8.8.8	192.168.2.7
Jan 28, 2022 10:58:45.456741095 CET	64296	53	192.168.2.7	8.8.8.8
Jan 28, 2022 10:58:45.480979919 CET	53	64296	8.8.8.8	192.168.2.7
Jan 28, 2022 10:58:50.542371035 CET	58820	53	192.168.2.7	8.8.8.8
Jan 28, 2022 10:58:50.569107056 CET	53	58820	8.8.8.8	192.168.2.7

DNS Queries

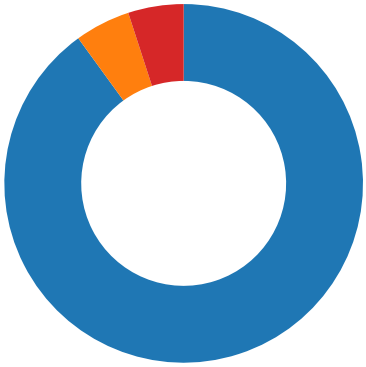
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 10:58:40.275278091 CET	192.168.2.7	8.8.8.8	0x5b67	Standard query (0)	www.pointconstructionservices.com	A (IP address)	IN (0x0001)
Jan 28, 2022 10:58:45.456741095 CET	192.168.2.7	8.8.8.8	0x741d	Standard query (0)	www.amr-fire.net	A (IP address)	IN (0x0001)
Jan 28, 2022 10:58:50.542371035 CET	192.168.2.7	8.8.8.8	0x7770	Standard query (0)	www.collective4choice.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 10:58:40.305191040 CET	8.8.8.8	192.168.2.7	0x5b67	No error (0)	www.pointconstructionservices.com	pointconstructionservices.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 10:58:40.305191040 CET	8.8.8.8	192.168.2.7	0x5b67	No error (0)	pointconstructionservices.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 28, 2022 10:58:45.480979919 CET	8.8.8.8	192.168.2.7	0x741d	No error (0)	www.amr-fire.net	d1g9pg5cncourf.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 10:58:45.480979919 CET	8.8.8.8	192.168.2.7	0x741d	No error (0)	d1g9pg5cncourf.cloudfront.net		13.225.39.103	A (IP address)	IN (0x0001)
Jan 28, 2022 10:58:45.480979919 CET	8.8.8.8	192.168.2.7	0x741d	No error (0)	d1g9pg5cncourf.cloudfront.net		13.225.39.125	A (IP address)	IN (0x0001)
Jan 28, 2022 10:58:45.480979919 CET	8.8.8.8	192.168.2.7	0x741d	No error (0)	d1g9pg5cncourf.cloudfront.net		13.225.39.124	A (IP address)	IN (0x0001)
Jan 28, 2022 10:58:45.480979919 CET	8.8.8.8	192.168.2.7	0x741d	No error (0)	d1g9pg5cncourf.cloudfront.net		13.225.39.100	A (IP address)	IN (0x0001)
Jan 28, 2022 10:58:50.569107056 CET	8.8.8.8	192.168.2.7	0x7770	Name error (3)	www.collective4choice.com	none	none	A (IP address)	IN (0x0001)

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: HSBC Bank Swift Copy.pdf.exe PID: **4712**, Parent PID: **5696**

General

Target ID:	0
Start time:	10:56:23
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\HSBC Bank Swift Copy.pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\HSBC Bank Swift Copy.pdf.exe"
Imagebase:	0xe60000
File size:	770048 bytes
MD5 hash:	76B0F4441930D3F2F480830681C426E7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.308215845.0000000003258000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.307751069.00000000031A1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.308628609.00000000041A9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.308628609.00000000041A9000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.308628609.00000000041A9000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: HSBC Bank Swift Copy.pdf.exe PID: **4824**, Parent PID: **4712**

General

Target ID:	12
Start time:	10:56:48
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\HSBC Bank Swift Copy.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\HSBC Bank Swift Copy.pdf.exe
Imagebase:	0x810000
File size:	770048 bytes
MD5 hash:	76B0F4441930D3F2F480830681C426E7

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.378377402.0000000000E50000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.378377402.0000000000E50000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.378377402.0000000000E50000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.378466176.00000000011A0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.378466176.00000000011A0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.378466176.00000000011A0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000000.304686882.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000000.304686882.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000000.304686882.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000000.304254698.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000000.304254698.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000000.304254698.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.377961712.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.377961712.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.377961712.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4186C7	NtReadFile

Analysis Process: explorer.exe PID: **3292**, Parent PID: **4824**

General

Target ID:	14
Start time:	10:56:52
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000000.339842712.000000000B7CD000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000000.339842712.000000000B7CD000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000000.339842712.000000000B7CD000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000000.356870466.000000000B7CD000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000000.356870466.000000000B7CD000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000000.356870466.000000000B7CD000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: svchost.exe PID: 5976, Parent PID: 3292

General

Target ID:	17
Start time:	10:57:20
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x1210000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.531069292.0000000000F50000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.531069292.0000000000F50000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.531069292.0000000000F50000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.528571201.00000000008F0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.528571201.00000000008F0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.528571201.00000000008F0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.532271564.0000000000F80000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.532271564.0000000000F80000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.532271564.0000000000F80000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	9086C7	NtReadFile

Analysis Process: cmd.exe PID: 4384, Parent PID: 5976

General

Target ID:	19
Start time:	10:57:25
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\HSBC Bank Swift Copy.pdf.exe"

Imagebase:	0x870000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5464, Parent PID: 4384

General

Target ID:	20
Start time:	10:57:26
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 4524, Parent PID: 568

General

Target ID:	29
Start time:	10:58:01
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	explorer.exe
Imagebase:	0x7ff662bf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly